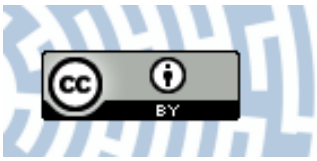
Title: Ochrona stacji roboczych w Uniwersytecie Śląskim : w oparciu o zaawansowane technologicznie rozwiązania sprzętowe i programowe

Author: Andrzej Koziara, Barbara Wróbel



Andrzej Koziara

Barbara Wróbel
Oddział Obsługi Informatycznej
Bibliotek Uniwersytetu Śląskiego

Ochrona stacji roboczych w Uniwersytecie Śląskim - w oparciu o zaawansowane technologicznie rozwiązania sprzętowe i programowe

Wstęp

Wszystkie systemy komputerowe były, są i będą podatne na wszelkiego rodzaju awarie, wynikające nie tylko z zawodności sprzętu i oprogramowania, ale również ze świadomych i nieświadomych działań ich użytkowników. Chcąc ograniczyć ich najczęściej katastrofalne następstwa, podjęto w minionych latach wiele działań zmierzających do opracowania koncepcji redukujących występowanie szkód. Skoncentrowano się w nich głównie na próbie ograniczenia prawa użytkownika do ingerencji w system. Jako standardowe, tak dla pojedynczych stacji roboczych, jak i systemów sieciowych, stało się ograniczanie możliwości wykonywania pewnych operacji przez ich użytkowników.

Jednym z najbardziej znanych mechanizmów implementujących taką właśnie strategię w stosunku do systemów sieciowych, stało się wykorzystanie Group Policy[1] na podbudowie Active Directory[2]. Stworzenie z ich wykorzystaniem odpowiednich zasad zabezpieczeń dla sieci, zwykle jest kolosalnym przedsięwzięciem, wymagającym dużo wysiłku ze strony administratora. Rodzi się tylko pytanie, czy w każdej sytuacji koniecznym? Tym bardziej, że zastosowanie niektórych zasad zabezpieczeń nie zawsze jest możliwe w starszych systemach, jak np. Windows 98. Poza tym nawet, jeżeli zostało zainstalowane odpowiednie oprogramowanie antywirusowe, nigdy nie ma 100% pewności, iż któryś z nowych (a jeszcze nieuwzględnionych w bazie programu antywirusowego) wirusów nie spowoduje awarii systemu. Równocześnie zauważono, że stosowanie sztywnych reguł zabezpieczeń jest właściwe, gdy mamy do czynienia ze stałym przypisaniem funkcji użytkowych do stanowisk roboczych lub grup użytkowników. Sytuacja ta jest całkowicie sprzeczna z warunkami, jakie musimy stworzyć dla czytelników bibliotek odwiedzających nasze czytelnie oraz pracownie komputerowe. Gwałtowny rozwój technik informatycznych i sposobów pracy źródeł internetowych wymusza zmianę podejścia do zagadnienia zabezpieczeń z modelu "zezwalam na....." na model "wszystko, co nie jest zakazane, jest dozwolone".

Zaczęto, więc poszukiwać nowych rozwiązań, które uprościłyby administrację, szczególnie w środowiskach najbardziej podatnych na różnego rodzaju zagrożenia ze strony użytkownika, jak i wirusów.
Mimo wysokich kwalifikacji kadr informatycznych, pracujących w bibliotekach, informacje, które mogą one pozyskać ze źródeł tradycyjnych i elektronicznych, są tak skąpe, że do dnia dzisiejszego w zdecydowanej większości bibliotek są stosowane rozwiązania, które dla Uniwersytetu Śląskiego stały się niewystarczające już cztery lata temu. Typowym, do dnia dzisiejszego, jest wykorzystywanie oprogramowania Ghost firmy Symantec.

Oprogramowanie to zostało użyte w Bibliotece Politechniki Świętokrzyskiej, a jego wykorzystanie scharakteryzowano jako możliwość zdalnego i cyklicznego odświeżenia konfiguracji publicznych komputerów[3]. Jak wykazały doświadczenia zespołu administratorów wydziałów, instytutów oraz bibliotek Uniwersytetu Śląskiego tak prowadzone odświeżanie jest bardzo uciążliwe, kosztowne i ponad miarę angażujące osoby odpowiedzialne za stan dostępnych publicznie stacji roboczych. Z naszych doświadczeń wynikało, że administratorzy wydziałowych i instytutowych pracowni informatycznych "odświeżali" stanowiska prawie po każdej turze zajęć, natomiast w bibliotekach odbywało się to minimum raz do kilku razy dziennie (przy czasie odtwarzania rzędu kilkunastu minut). Dlatego też z ulgą powitaliśmy doniesienia w zagranicznej prasie informatycznej, że podjęto prace nad systemami, które te czynności mogą w pełni zautomatyzować. Równocześnie dostrzegliśmy, że rozwiązania tam są unikalne, co jednoznacznie sugeruje, że stosowane technologie objęte są ochroną patentową. Do prac nad rozwiązaniem tego problemu włączyły się tak firmy produkujące podzespoły komputerowe, jak i te, które zajmują się tylko produkcją oprogramowania. Efektem tych prac stały się:

- zabezpieczenia sprzętowe, oparte o karty wkładane w sloty ISA (produkowane w latach 2001-2002) lub PCI;
- zabezpieczenie przy pomocy oprogramowania instalowanego w gotowych systemach operacyjnych rodziny Windows.

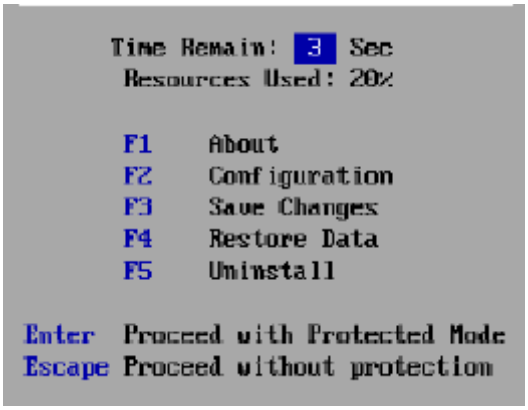
Możliwości kart zabezpieczających

Karty te należą do rodziny elementów wkładanych do komputerów osobistych w najbardziej typowe w ciągu ostatnich lat złącza PCI (tak jak inne karty stanowiące części komputera, np.: karta sieciowa, dźwiękowa czy modem). Wykonywane są w różnych odmianach, a wizualnie i funkcjonalnie możemy podzielić je na dwie grupy: te wyposażone w kartę sieciową oraz te, które tej funkcjonalności nie posiadają. Charakterystyczną ich cechą jest to, że w swoim działaniu pozwalają na natychmiastowe przywrócenie danych i stanu systemu do wartości wzorcowych. Tym samym działanie ich polega na automatycznym wycofaniu wszystkich zmian dokonanych celowo lub przypadkowo przez użytkownika, wirusy komputerowe, a nawet utraconych na skutek formatowania dysku. Karty te dostępne są w kilku wariantach: PCI 2000, WOL 2000, Extra oraz Professional. Wszystkie one wspierają (zapewniają prawidłową pracę) systemy operacyjne: Windows 95, 98, Me, 2000, XP, a wybrane z nich DOS, Windows 3.x czy też jak to ma miejsce w przypadku Extra Linux oraz Novell. Obsługują również najbardziej powszechne standardy dyskowe (IDE, SSCI, EIDE, ATA, SATA)[4] oraz systemy plików (FAT16, FAT32, NTFS)[5]. Szczegółowe opisy poszczególnych kart, głównie w wersjach anglojęzycznych, znajdują się na stronie ich producentów, których adresy można pozyskać na podstawie wyszukiwań wykonywanych przy pomocy systemów wyszukiwarek światowych lub na podstawie artykułów dostępnych w światowych i polskich czasopismach informatycznych.

Ze względu na bardzo szeroki wachlarz ich cech, których analiza wymagałaby zapewne kilkudziesięciu stron, w artykule skoncentrujemy się na najbardziej kluczowych i podstawowych ich właściwościach. Zanim rozpoczniemy omawianie szczegółowych funkcjonalności, jakie oferują nam karty, warto zwrócić uwagę, że niektóre z nich mają wbudowaną kartę z interfejsem sieciowym. Interfejsy te dają możliwość uruchamiania funkcji przenoszenia obrazów dysku podobnej do rozwiązań oferowanych chociażby przez wspomniany powyżej program Ghost firmy Symantec. Działanie tej funkcji polega na przenoszeniu poprzez sieci "obrazu" dysku twardego w całości, co za tym idzie umożliwia nam szybkie klonowanie systemów operacyjnych z zainstalowanymi aplikacjami użytkowymi na wiele komputerów. Oczywiście w czasie, gdy użytkujemy już systemy operacyjne z rodziny Windows XP, istnieje wiele przeciwwskazań przed używaniem tej funkcjonalności.
Mimo dużych różnic dla poszczególnych ich wykonań każda z nich działa w dwóch trybach:

- "protected" - zwany trybem chronionym; jest to standardowy tryb pracy karty, w którym utrzymywana jest niezmieniona konfiguracja dysku i chronione dane mogą być przywrócone po restarcie;

- "without protection" - zwany trybem otwartym czy też administracyjnym, w którym wszystkie zmiany w systemie operacyjnym są trwałe, a dane nie są w żaden sposób chronione. Tryb ten zwykle jest wykorzystywany przez administratora dla zadań specjalnych takich, jak: instalowanie, odinstalowywanie czy też uaktualnianie oprogramowania. Wejście w ten tryb jest chronione hasłem.



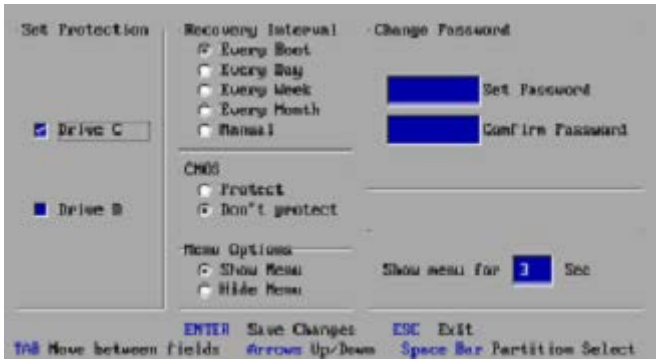
Rys. 1. Typowy panel karty

Dostęp do obydwu trybów możliwy jest poprzez panel pojawiający się podczas startu systemu (rys.1). Formatka ta pozwala również na odwołanie się do wszystkich pozostałych opcji karty, takich jak:

- "Save changes" - przydatny w przypadku, gdy dokonamy zmian, znajdując się w trybie "protected", a mimo to chcielibyśmy, by zostały zachowane przy kolejnym restarcie komputera;
- "Restore Data" - używany w sytuacji, gdy chcemy przywrócić dysk do ostatnio zachowanego stanu;
- "Configuration" - ustawienia konfiguracji karty.

Ostatnia z wymienionych opcji stanowi, jak sama nazwa wskazuje, centrum kontroli konfiguracji karty. Dostęp tam, podobnie jak w przypadku trybu otwartego, jest zarezerwowany tylko dla znającego hasło administratora, co przeciwdziała wprowadzeniu jakichkolwiek niepożądanych modyfikacji przez nieuprawnionych użytkowników stacji roboczej.

Doświadczenia nabyte podczas konstruowania pierwszych wersji kart doprowadziły do sytuacji dzisiejszej, gdzie przejrzyste rozmieszczenie poszczególnych opcji jak gdyby z góry sugeruje przebieg jej konfiguracji wskazując opcje domyślne (rys.2).



Rys. 2. Formatka konfiguracyjna ustawień karty

Pierwszym elementem jest ustawienie w sekcji "Set protection" partycji, które będą przywracane przez kartę. Maksymalna ich ilość zależna jest od rodzaju posiadanej karty, ale już nawet najbardziej ubogie modele kart zapewniają rozpoznawanie i ochronę do ośmiu partycji. Zdrowy rozsądek wskazuje na to, że nawet przy największych

współcześnie spotykanych dyskach twardych jest to liczba w zupełności wystarczająca.

Jednakże, pomimo rysującej się możliwości zabezpieczenia praktycznie wszystkich partycji dyskowych, dobrze jest wziąć pod uwagę pozostawienie jednej z nich jako niechronionej. Partycja ta może posłużyć jako miejsce trwałego (niezależnego od restartów komputera) przechowywania danych użytkowników stacji roboczej. Jest to szczególnie użyteczne w przypadku, gdy system operacyjny lub program użytkowy ulegnie zawieszeniu, co wymusi na nas konieczność restartu komputera. W zależności od rozwiązań regulaminowych, dane z takiej niechronionej partycji usuwa sam użytkownik lub jest to wykonywane przez bibliotekarzy obsługujących czytelnie.

Kolejnym elementem w konfiguracji karty jest określenie interwałów czasowych przywracania systemu. Może się to odbywać raz dzienne, raz w tygodniu, raz w miesiącu, ale również możemy wybrać ręczne przywracanie stanu systemu (poprzedzone oczywiście uwierzytelnieniem przez podanie hasła), czy też automatyczne, wykonywane przy każdym restarcie systemu. Jak się wydaje, w zastosowaniach, z którymi mamy do czynienia w naszych bibliotekach, ustawienie "automatyczne przywracanie systemu przy każdym restarcie" jest opcją najczęściej wybieraną przez administratorów. Dzieje się tak, dlatego że każdy z kolejnych użytkowników stanowiska komputerowego powinien rozpocząć na nim pracę, posiadając w pełni stabilny i czysty system operacyjny. Równocześnie należy zauważyć, że każdy restart komputera "naprawia" system operacyjny bez konieczności wzywania administratora.

W obrębie panelu konfiguracyjnego karty posiadamy również pola służące definiowaniu hasła zabezpieczającego ustawienia karty, jak też wykonywanie zmian w samym systemie operacyjnym stacji roboczej. Karta daje także możliwość ochrony przed nieuprawnionymi zmianami nie tylko samych danych zapisanych na dyskach twardych, ale również pomaga zapobiegać ewentualnym ingerencjom w CMOS komputera (wywoływanym poza kontrolą użytkownika, np. przez pewne odmiany wirusów).

Podsumowując dotychczasowe rozważania, warto zwrócić uwagę na jeszcze jeden istotny aspekt dotyczący kart, a mianowicie ich niewielkie wymagania sprzętowe. Karty WOL 2000 i Extra działają już od procesorów 80386, natomiast pozostałe modele w komputerach z procesorami 80486 i wszystkich rodzajach Pentium. Ponadto algorytm kodujący dane i zezwalający na ich przywracanie dla swego działania wymaga zaledwie 1% wolnej powierzchni dyskowej. Dzieje się tak dlatego, że algorytm kodujący jest zaszyty w samej karcie, natomiast dysk twardy jest wykorzystywany tylko do zapisu danych. Tak rozwiązana kwestia zapisu z jednej strony jest zaletą (awaria karty nie powoduje utraty danych), z drugiej jednak strony determinuje fakt, że wykorzystanie kart nie jest panaceum na wszelkiego rodzaju awarie. Stosując je do ochrony systemu operacyjnego, nie zapobiegniemy utracie danych na skutek fizycznego uszkodzenia dysku.
Kolejną ogromna zaletą kart jest zadziwiająco szybki proces przywracania systemu trwający nawet kilka, nieraz kilkanaście sekund. Ta szybkość działania w starych i słabych komputerach sprawia, że praktycznie żadne rozwiązanie programowe nie jest w stanie jej na tym polu dorównać.

Koncepcja wykorzystania oprogramowania do ochrony zasobów

Pomimo wszystkich powyżej omawianych zalet kart, rynek ich zastosowania w ciągu ostatnich dwóch lat uległ znacznemu ograniczeniu. Zasada jej działania oparta jest na pełnej integracji i współdziałaniu z rozwiązaniami stosowanymi na płytach głównych stanowisk komputerowych. Stąd też, niestety, realna stała się sytuacja z początku 2004 roku, w której karta odmawia współpracy z niezgodnym ze sobą sprzętowo nowym modelem płyty głównej. Jeszcze dziwniejszy był dalszy ciąg tej sprawy. Po przeprowadzeniu testów okazało się, że z tym konkretnym modelem płyty głównej (zresztą dobranej bardzo starannie pod względem producenta, możliwości, stabilności, a nawet 3-letniej gwarancji) w miarę prawidłowo współpracowały karty w wersjach niższych o 2 i 3 poziomy, natomiast starsze znów nie. Stąd też grono administratorów sieciowych Uniwersytetu Śląskiego w tej dziedzinie zabezpieczeń, skierowało uwagę na rozwiązania typowo programowe. Główną przesłanką, która skierowała nasze kroki w tym kierunku, była konieczność dobrania systemu zabezpieczania stacji roboczych,

niezależnego od wewnętrznych cech zastosowanych podzespołów.

Dokonaliśmy przeglądu rynku, korzystając ze źródeł podobnych, jakie stosowaliśmy w czasie poszukiwania kart (zagraniczna prasa informatyczna i systemy wyszukiwarek internetowych), oraz wybraliśmy produkt, który w swojej minimalnej wersji zapewnia kontrolę zasobów identyczną do rozwiązań sprzętowych.

Programowe narzędzie ochrony zawartości dysków

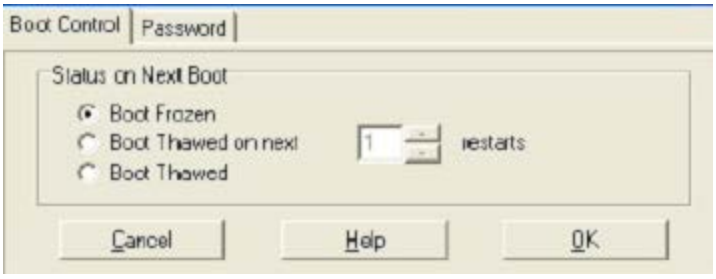
Podstawowym celem zastosowania oprogramowania jest zastąpienie niezbyt pewnie działających kart w komputerach nowej generacji. Podobnie jak karty ma on chronić systemy operacyjne stacji roboczych przed wszelkimi niepożądanymi zmianami.

Oprogramowanie, które wybraliśmy na potrzeby Uniwersytetu Śląskiego, dostępne jest w trzech wersjach: Standard, Professional i Enterprise. Wybór pomiędzy nimi uwarunkowany jest przede wszystkim rozmiarem środowiska, które program ma ochraniać, ułatwiając jednocześnie administratorowi (czy też administratorom) kontrolę nad coraz bardziej liczną i złożoną strukturą sieci oraz systemów komputerowych. Dla zobrazowania tego, co powinniśmy poszukiwać dla wersji minimalnych, omówimy jak najbardziej istotne dla nas cechy stosowanego przez Uniwersytet Śląski oprogramowania.

Możliwości wersji Standard

Wersja Standard, jak sama nazwa wskazuje stanowi podstawową i zarazem najbardziej okrojoną wersję oprogramowania stosowanego na Uniwersytecie Śląskim. Dokładne omówienie jej możliwości stanowi bardzo dobry punkt wyjściowy do późniejszego zaprezentowania uzupełnień, jakie zostały wprowadzone do dwóch kolejnych wariantów produktu.

Podobnie jak w przypadku kart, program w wersji Standard ma wsparcie dla podstawowych systemów operacyjnych Microsoft (Windows 95, 95, Me, 2000, XP), głównych systemów plików (FAT, NTFS) oraz standardów dyskowych (IDE, SCSI, ATA, SATA). Podczas instalacji można nie tylko określić partycje, które będą podlegać ochronie (co jest określane w programie mianem zamrożenia), ale również znane administratorowi hasła dostępu do konfiguracji oprogramowania. Hasło to wymagane jest również przy odmrażaniu systemu, czyli zdejmowaniu ochrony partycji. Ochrona ta może być wycofana na stałe, jak również na określoną ilość startów systemu (rys.3).



Rys. 3. Kontrola startów systemu

Oprogramowanie to od chwili ustawienia omówionych powyżej parametrów pozwala na automatyczne odzyskiwanie zasobów przy każdym starcie systemu, zapobiegając wprowadzaniu trwałych zmian przez użytkowników. Aby stwierdzenie to było w 100% prawdą, niezbędne jest zwrócenie uwagi na spełnienie dodatkowych warunków. Podstawowym z nich jest odebranie użytkownikom możliwości bootowania (startowania) komputera ze stacji dyskietek lub czytnika nośników optycznych (CD-ROM, DVD-ROM) poprzez zablokowanie tych funkcji w BIOS stacji roboczej. Należy bowiem zdać sobie sprawę z tego, że oprogramowanie to działa z poziomu systemu operacyjnego Windows i dopiero po jego uruchomieniu chroni dane zapisane na dyskach twardych. Wystartowanie komputera z dyskietki lub CD powoduje, że system Windows, a co za tym idzie oprogramowanie to, nie zostaje uruchomione, a to w rezultacie pozwala na dokonanie

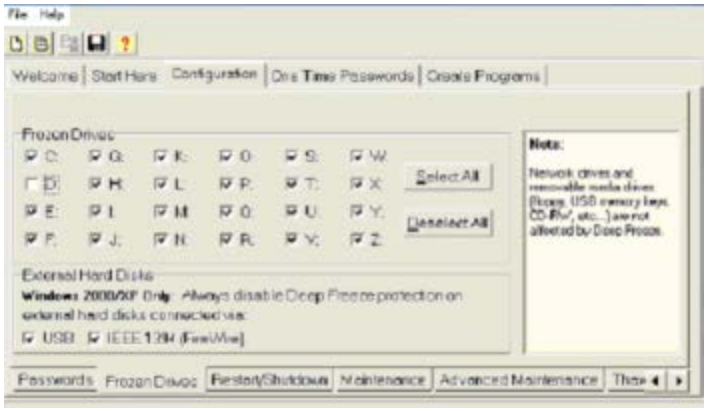
dowolnych stałych zmian na dyskach (łącznie z jego sformatowaniem). Jeżeli jednak spełnimy wymóg wskazania jedynego źródła startu systemu operacyjnego na dysk twardy oprogramowanie, podobnie jak karty, pozwoli na całkowitą i sprawną ochronę systemu operacyjnego oraz danych zapisanych na wskazanych do ochrony partycjach (również przed wirusami).

Dodatkowe funkcjonalności w wersjach Professional i Enterprise

Kolejne wersje tego oprogramowania - Professional i Enterprise zawierają dodatkowe funkcje wzbogacające opisane powyżej cechy wersji Standard. Główną zaletą obydwóch jest wyposażenie ich w konsole administracyjne sterujące wszystkimi funkcjami przez nie posiadanymi. Równocześnie centra te pozwalają w wygodny sposób tworzyć własne pakiety instalacyjne, które następnie wykorzystujemy podczas instalacji oprogramowania na stacjach roboczych. Dzięki zastosowaniu tzw. "Customization Code" zapewniają również pełne bezpieczeństwo generowanych przez nie pakietów instalacyjnych. Kod ten daje gwarancję, że wygenerowanie poprawnego hasła dla stacji roboczej będzie możliwe tylko i wyłącznie w centrum administracyjnym, którego "Customization Code" jest zgodny z kodem użytym podczas kreowania danego pakietu.

Zgodność tegoż kodu będzie również miała znaczenie przy kontroli stacji poprzez Konsolę Administracyjną (szerzej opisaną w dalszej części artykułu) zaimplementowaną w wersji Enterprise. Kod ten jest też wymagany w przypadku powtórnej instalacji systemu operacyjnego komputera, na którym znajduje się centrum administracyjne. Wykorzystujemy go również podczas przenoszenia centrum administracyjnego na inny komputer. Wtedy to staje się on niezbędny w celu zapewnienia dalszej, nieprzerwanej kontroli stacji, na których zainstalowano pakiety oprogramowania ochronnego wygenerowane w oparciu o niego. Wykorzystując możliwość generowania spersonalizowanych pakietów instalacyjnych, zmniejszamy znacząco nakład pracy przypadającej na instalację oprogramowania ochronnego w całej sieci komputerowej naszej uczelni. Oszczędzając czas administratora, jednocześnie eliminujemy ewentualne możliwe pomyłki, do których mogłoby dojść podczas konfiguracji oprogramowania ochronnego na poszczególnych stacjach.

W tworzonym centralnie pakiecie instalacyjnym administrator tylko raz określa konfigurację poszczególnych elementów oprogramowania. Zapewne najważniejszym z nich jest określenie dysków podlegających zamrożeniu (rys. 4). Można tu nawet wygenerować wirtualną partycję o określonym rozmiarze, która nie będzie przywracana podczas startu systemu, pozwalając dzięki temu na trwałe przechowywanie danych.



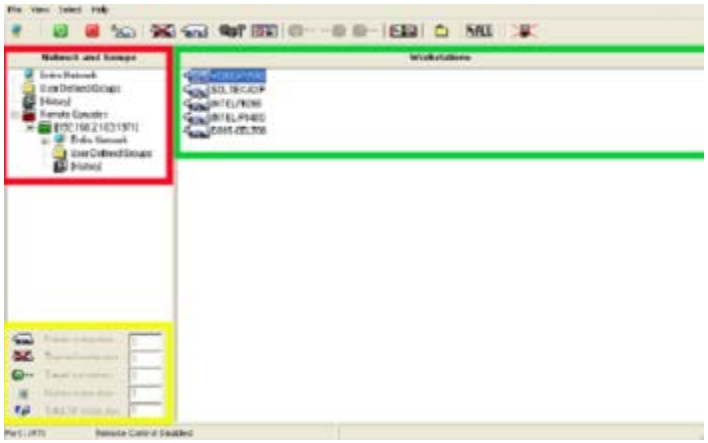
Rys. 4. Wybór chronionych partycji

Kolejną kluczową sprawą dla administrowania systemami informatycznymi w dużych instytucjach (duże wydziały czy biblioteki) jest ustalenie haseł dostępu, których w przypadku wersji Professional może być 4, a w wersji Enterprise aż 15. Umożliwia to przyznanie dostępu dla wielu administratorów i obsługę z poziomu jednej konsoli całego kampusu lub nawet całej uczelni. Wersja Enterprise idzie jeszcze dalej, ponieważ pozwala na ustalenie przedziału czasu, w którym hasła będą aktywne. Dla zapewnienia wysokiego poziomu bezpieczeństwa zarządzania systemami przewidziano również awaryjną furtkę

na wypadek utraty hasła przez administratora (np. na skutek zapomnienia czy dłuższej nieobecności).W przypadku wystąpienia takiej potrzeby można je wygenerować, korzystając z zakładki "One Time Passwords". Hasło generowane jest na podstawie tokenu stacji (indywidualny identyfikator stacji roboczej) oraz "Customization Code" centrum administracyjnego. Może to być zarówno hasło jednorazowe, jak i hasło jednodniowe przeznaczone do wielokrotnego użycia.

Jak więc widzimy zarówno karty, jak i oprogramowanie dość kompleksowo chronią partycje przed dokonywaniem jakichkolwiek zmian ich zawartości. Chronią również, a może przede wszystkim partycję systemową, co wbrew pozorom nie zawsze jest zjawiskiem korzystnym. Staje się wręcz problemem w przypadku konieczności systematycznej instalacji elementów uzupełniających, jak np. poprawki systemowe. Oprogramowanie Professional i Enterprise rozwiązuje tę kwestię poprzez zaimplementowanie tzw. harmonogramu konserwacji. Określa on, w jakich dniach i godzinach mają odbywać się zaplanowane restarty systemów operacyjnych stacji roboczych. Możemy również zdefiniować, w jakich przedziałach czasowych systemy mają pozostawać odblokowane, by można było dokonać trwałych zmian w ich konfiguracji, np. wykorzystując Windows Updates czy automatyczne uzupełniania bazy wirusów w programach antywirusowych.

Pomimo wielu zbieżnych funkcjonalności wersji Professional i Enterprise, bez wątpienia najciekawszą z punktu widzenia administratora systemów pozostaje Enterprise. W wersji tej nie poprzestaje się na automatyzowaniu procesu generowania plików instalacyjnych dla stacji roboczych. Jej priorytetowym celem staje się zapewnienie zdalnej kontroli nad zarządzanymi przez nie komputerami. Osiągamy to poprzez generowanie tzw. "Workstation Seed", pełniących na stacjach roboczych funkcję agentów systemu, oraz "Enterprise Console", będącą centrum koordynacji działania poszczególnych instalacji pełnej wersji oprogramowania ochronnego lub tylko jego agenta (rys.5).



Rys. 5. Konsola administracyjna

Agent "Workstation Seed" staje się minimalnym, wymaganym oprogramowaniem, koniecznym dla zdalnej kontroli stacji. Sam w sobie stacji nie chroni, ale dzięki jego działaniu możliwa staje się zdalna instalacja właściwego oprogramowania najczęściej poprzez pakiet "Full Workstation" dający pełną funkcjonalność systemową.

Konsola współpracując z zainstalowanymi na poszczególnych stacjach agentami, pozwala nie tylko na zainstalowanie oprogramowania klienckiego, ale również na ewentualne zdalnie wykonywane zmiany na poszczególnych stacjach. Eliminuje to konieczność fizycznej obecności administratora przy każdej stacji i ręcznego wykonywania niezbędnych modyfikacji. Po ich wykonaniu możliwe jest zdalne wyłączenie czy też zrestartowanie stacji w celu natychmiastowego wymuszenia zastosowania właśnie wykonanych zmian w konfiguracji.

Administrator poprzez swoją konsolę może również sprawdzać status oprogramowania chroniącego na poszczególnych stacjach, tzn. czy stacja jest obecnie chroniona, czy też nie, jak również stwierdzać, że stacja jest wyłączona.

Wszelkie zmiany dokonywane w statusie stacji znajdują swoje odzwierciedlenie w logu, który może stać się punktem wyjścia do późniejszych analiz procesu pracy oprogramowania ochronnego oddzielnie dla każdej stacji roboczej.

Konsola daje również możliwość logicznego pogrupowania stacji w celu jaśniejszego zobrazowania struktury sieci. Można więc powiedzieć, że z pozycji administratora w wersji "Enterprise" stanowi dosyć ciekawą alternatywną funkcję monitoringu i może stać się całkiem użytecznym narzędziem przeznaczonym do zarządzania całą siecią.

Podsumowanie

Reasumując, karty, jak i program o powyższych cechach, wydają się idealnym rozwiązaniem w przypadku środowisk o dostępie otwartym (takich jak np. czytelnie czy też pracownie bibliotek), w których użytkownicy dokonujący ingerencji w systemy komputerowe często są do tego nieuprawnieni i dlatego istnieje konieczność szybkiego oraz bezproblemowego cofnięcia dokonanych przez nich zmian - zmian, których źródłem mogą stać się również wirusy. Równocześnie dla zapewnienia pełnej funkcjonalności systemów administratorzy nie mogą tak skonfigurować systemów stacji roboczych, by zablokować na nich podstawowe funkcje administracyjne. Systemy przywracania stanu systemu operacyjnego mają również ogromne znaczenie dla właściwej konfiguracji pracowni szkoleniowych, gdzie niemożliwość wykonywania zmian stoi w sprzeczności z ich funkcjami, bo co to za szkolenie, jeśli użytkownik nie będzie mógł choćby zmienić czułości myszki, rozdzielczości ekranu czy innego ustawienia przeszkadzającego mu w wydajnej pracy i osiąganiu właściwych postępów merytorycznych.

Wybór pomiędzy tymi grupami rozwiązań zawsze musi być poprzedzony szczegółową analizą potrzeb, związanych nie tylko z bogactwem oferowanych przez oba rozwiązania funkcjonalności, ale również z możliwościami sprzętowymi stacji roboczych. Przy obecnym stopniu rozwoju technologii widać dość znaczne zacieranie się różnic wydajności pomiędzy rozwiązaniami programowymi a sprzętowymi, co tym samym zwiększa zakres wyboru i pozwala mówić o konkurencyjności obu produktów.

Przypisy

[1] Group Police - reguły określające, co i kiedy mogą wykonywać poszczególni użytkownicy na konkretnych komputerach.

[2] Active Directory - standard firmy Microsoft, przy pomocy którego układane są w logiczne ciągi reguły dostępu użytkowników do zasobów komputerów i sieci komputerowej (w tym globalnej sieci Internet).

[3] KARBOWNIK, M. Bezpieczna sieć komputerowa w nowoczesnej bibliotece na przykładzie Politechniki Świętokrzyskiej. In Biuletyn EBIB [on-line]. 2005 nr 5 (66) maj [dostępny 21 maja 2005]. Dostępny w World Wide Web: **http://ebib.oss.wroc.pl/2005/66/karbownik.php**, ISSN 1507-7187.

[4] Standardy złącz, jakimi w sposób fizyczny dyski twarde są włączane w komputerze do jego innych elementów.

[5] Sposoby logicznego opisu miejsca, gdzie na dysku twardym umieszczane są katalogi lub zapisywane są poszczególne pliki.

Bibliografia

1. Opis niezależnego testu redakcji Chip PL dane z witryny internetowej czasopisma Chip Online: ZIELIŃSKI, T. Chronić twardziela. In Chip Online [on-line]. [dostęp 15 kwiecień - 22 kwiecień 2005]. Dostępny w World Wide Web: **http://www.chip.pl/arts/archiwum/kth/kthar_18575.html**.

2. Witryna z recenzjami technologii informatycznych: Bitpipe [on-line]. [dostęp 15 kwiecień - 22 maja 2005]. Dostępny w World Wide Web: **http://www.bitpipe.com**.

3. Witryna z recenzjami technologii informatycznych: techLEARNING [on-line]. [dostęp 15 kwiecień - 22 maja 2005]. Dostępny w World Wide Web: http://www.techlearning.com.

4. Dokumentacja fabryczna "User Guide" firmy Faronics do rodziny systemów "Deep Freeze", sierpień 2004.

5. Opis techniczny kart "Magic Card" na witrynie internetowej producenta sprzętu: Magiccard [on-line]. [dostęp 15 kwiecień - 22 maja 2005]. Dostępny w World Wide Web: http://www.rogev.com/.

6. Opis techniczny oprogramowania "Deep Freeze" na witrynie internetowej producenta sprzętu: Faronics [on-line]. [dostęp 15 kwiecień - 22 maja 2005]. Dostępny w World Wide Web: http://www.faronics.com/.